5 EXAMPLES OF IT NETWORK OUTAGES

Service outage is a reality that enterprise IT must deal with. In the age of cloud computing and connected networks, vendors and customers rely on redundant systems, backups and a range of disaster mitigation systems to reduce the risk of an IT outage. Yet, the biggest cloud outages are dominated by pioneers of cloud infrastructure technologies that power most of the technology-driven business organizations around the world.

Here are examples of 5 IT network, cloud or datacenter outages that occurred in 2018:

1. Amazon Web Services, March 2018

A year after the massive AWS S3 outage of February 2017, AWS customers including critical enterprise IT solutions providers Atlassian, Slack and Twilio experienced downtime in March 2018. This time, the outage had hit the AWS-East Region and affected several applications relying on the AWS servers at its Ashburn, Virginia data center space. The AWS Availability Zone of Ashburn serves as a major networking infrastructure hub for connectivity services providers across the nation. In particular, the outage impacted customers of the AWS Direct Connect customers in the US-East-1 Region. The root cause of the issue was a power outage that translated into elevated latency, packet loss or downtime for Internet users relying on the AWS Direct Connect service. Additionally, the downtime also appeared to have impacted the company's own voice assistance service, Alexa.

Similar issues resurfaced in May, when power failure in the North Virginia region data centers caused hardware failures. The impacted services included AWS EC2, database, data warehousing and

virtual desktop services. Later in July on the Amazon Prime day, the peak sales duration for the Amazon.com ecommerce site, the service experienced an outage for six hours out of the 36 hour record-breaking promotional sales event. This time however, the outage was tied to a software issue and not the underlying AWS cloud infrastructure itself.

2. Microsoft Azure, June 2018

2018 saw the warmest summers in the Nordics, the region that is widely popular among cloud service providers due to virtually limitless free cooling available for data center hardware. Microsoft Azure therefore experienced outage in the Ireland region when the temperature reached an otherwise pleasant 18°C or 64°F. The temperature was a little too much for the region forecasting water shortage for the residents, leaving Microsoft with inadequate cooling supply to operate its Dublin data center resources at optimal temperature. As a result, the data center service experienced an outage for around 9 hours, affecting Azure and Office 365 customers in the Northern European countries.

This was not the only weather-induced outage facing the Microsoft Azure cloud service in the year. A lightning strike caused interruption in the company's San Antonio, Texas data center and affected Azure and Office 365 customers in the South Central US region in September 2018. The weather incident impacted the cooling system of the data center, which forced the hardware shutdown and restart to prevent further damage excessive and uncontrollable heat in the infrastructure.

3. Google Cloud, July 2018

Like all major cloud service providers, Google has had its fair share of issues delivering infrastructure services to an exploding customer-base. The affected services included the Google App Engine, Stackdriver, Diagflow and Global Load Balancers. Customer including Spotify, Discord, Pokemon Go app and Snapchat rely on these cloud networking services to reach a global audience, thereby cascading the impact globally. The outage lasted for around 30 minutes and up to 87 percent of the customers experienced some form of errors on the App Engine, HTTPS Load Balancer or the TCP/SSL Proxy Load Balancer solutions. According to a detailed description by Google, the issue was caused due to a bug in the new security feature added Google Front Ends (GFE) architecture layer. The bug had not been identified earlier despite extensive testing procedures in place, and was triggered only when the configuration changes were introduced in the production environment.

The affected customers were provided credits refund as per the Service Level Agreement (SLA) as a common compensation by any cloud vendor. However, the true cost of data center downtime that averages around $750,000 as of 2015 according to a Ponemon Institute research report far outweighed the offered compensation.

4. O2 Outage, December 2018

In terms of scale, the largest network outage impacted customers of O2 3G and 4G mobile services in the UK. The outage starting early hours on the December 6, 2018 left 30 million users without the Internet connectivity capabilities. The outage lasted the entire day and was caused due to failure on networking equipment operated by Ericsson and served to several carriers globally. Considering the scale of the issue, Ericsson readily worked to fix the issue and decommission the faulty software later on. Detailed analysis showed that the root cause was tied to expired certificate versions linked

to customers including O2. Telecommunication services relies on security certificates to verify the legitimacy of network traffic routing and security decisions performed at various layers of the communication infrastructure. Once the cause was isolated, the services were quickly restored across all users. O2 had previously suffered a network outage affecting millions of users in October 2018, although the issue lasted only 40 minutes.

5. CenturyLink, December 2018

The CenturyLink incident was the highlight network outage of 2018 as it left millions of users without the ability to call 911, ATM withdrawals, access to sensitive patient healthcare records, Verizon mobile data services and even lottery drawings. The incident later led to an FCC investigation considering the “unacceptable” downtime impacting emergency services such as 911 or ATM withdrawals. The outage lasted two days and was caused due to an issue with a single network management card. The device was found transmitting invalid data frame packets across the infrastructure. Despite the multiple layers of redundancy in place, the issue cascaded across its nationwide communication infrastructure. Once the infrastructure systems crashed, CenturyLink had limited visibility into its network to troubleshoot the issue.

Networking services are inherently interlinked across multiple large enterprises taking advantage of vast, distributed data center resources to reach a global audience. Once the backend infrastructure service goes down, the impact is reflected across the vast userbase, potentially impact critical services at a large scale.